Cassandra Crossing/ Altro che Immuni, Bluetooth spento!

(456) L'exploit BIAS del protocollo Bluetooth mette a rischio qualsiasi cellulare, e non è rimediabile.

Cassandra Crossing/ Altro che Immuni, Bluetooth spento!

(456) L'exploit BIAS del protocollo Bluetooth mette a rischio qualsiasi cellulare, e non è rimediabile.

28 maggio 2020—Ci sono delle notizie che navigano e vivacchiano sulla superficie dell'Infosfera senza mai finire nel mainstream.
Nemmeno in quello di un settore specialistico come la sicurezza informatica. Anche a non essere paranoici verrebbe da chiedersi come questo sia possibile…

La notizia è che il protocollo Bluetooth contiene una falla che permette di "impersonare" un device durante la fase di pairing di un dispositivo.
In pratica, dopo aver "accoppiato" il vostro cellulare con un auricolare, la vostra auto od il cellulare di un amico, è possibile che un altro device "maligno" sostituisca la connessione memorizzata e diventi uno dei vostri collegamenti Bluetooth permanenti ed "affidabili".
E da qui si apre un nuovo mondo per l'insicurezza informatica.

Una presentazione tecnica è reperibile qui, e la paper originale qui.

Il NIST lo classifica "solo" come bug di medio livello, ed anche questa classificazione è questionabile, almeno secondo Cassandra.

Infatti non stiamo parlando di un bug software, evento comunissimo e con cui siamo ormai familiari, rimediabile più o meno facilmente con una patch del software o del sistema operativo.

Non stiamo parlando nemmeno di una molto più grave falla nel silicio, come Meltdown delle CPU Intel, o Checkm8 della boot ROM dei cellulari iOS, che può talvolta essere mitigato oppure deve "corretto" con la dolorosa, ma al limite possibile, sostituzione del device.

BIAS è un bug del protocollo Bluetooth, cioè della specifica tecnica che definisce come i device Bluetooth devono comportarsi. Non è rimediabile in assoluto.

Parafrasando Lessig, "*… è una legge sbagliata del cyberspazio*".

E' sbagliata la legge, non c'è rimedio, non c'è mitigazione, non c'è patch, se non fare una nuova legge … per il lontano futuro.
Un nuovo protocollo richiede infatti anni per essere discusso, approvato e poi utilizzato in device reali.

Tuttavia, come in tante cose non indispensabili della vita tipo facebook, il rimedio in realtà esiste; farne a meno od usarlo il meno possibile.

Quindi "spegnere" il protocollo Bluetooth interamente, "accenderlo" sono quando serve, cancellare tutte le nuove connessioni appena non sono più necessarie.

E questo è il consiglio, banale, di Cassandra.

Certo questo renderà impossibile usare il contact tracing digitale, che si basa appunto su Bluetooth, e richiede che questo sia sempre acceso.

Ma il non poter usare Immuni ed i suoi succubi sarà, secondo l'opinione di Cassandra, un guadagno, non una perdita.

La cosa positiva che può scaturire da questa storia è che sia lo spunto per una riflessione ed un ragionamento, su **quanto siamo dipendenti da tecnologie che noi non comprendiamo,** e che anche gli esperti che le hanno realizzate non capiscono evidentemente fino in fondo.

Forse tutti noi dovremmo usarle, ed anche non usarle, con molto più senso critico.

Il che non significa non accettare una tecnologia ed i suoi rischi, purché siano noti e calcolati.

Proprio come hanno fatto i due astronauti che stanno per sedersi nella "Dragon", ed ai quali, per questo, vanno i personali ringraziamenti di Cassandra e dei suoi 24 lettori.

By Marco A. L. Calamari on May 31, 2020.

Canonical link

Exported from Medium on August 27, 2025.